

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

En-Seong Kang, et al.

Serial No.: *To Be Assigned*

Examiner: *To Be Assigned*

Filed: December 22, 1998

Art Unit: *To Be Assigned*

For: THE DIGITAL CONTENT ENCRYPTION APPARATUS AND METHOD  
THEREOF



**CLAIM OF PRIORITY**  
**UNDER 35 U.S.C. §119**

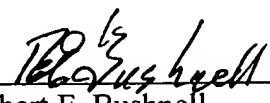
The Assistant Commissioner  
of Patents  
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application, Korean Priority No(s). 98-39808 and 98-39809 in Korea on 24<sup>th</sup> September 1998, and filed in the U.S. Patent and Trademark Office on December 22, 1998 is hereby requested and the right of priority provided in 35 U.S.C. §119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign applications.

Respectfully submitted,

  
Robert E. Bushnell  
Reg. No.: 27,774  
Attorney for the Applicant

1522 K Street, N.W.  
Suite 300  
Washington, D.C. 20005-1202  
Telephone: (202) 638-5740  
Telefacsimile: (202) 628-0755  
Folio: P55501  
Date: 12/22/98  
I.D.: REB/lj

# 대한민국 특허청

## KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto  
is a true copy from the records of the Korean Industrial  
Property Office.

출원 번호 : 1998년 특허출원 제39809호  
Application Number

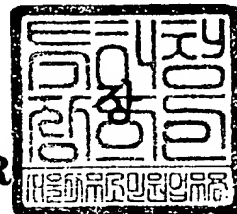
출원 년 월 일 : 1998년 9월 24일  
Date of Application

출원 인 : 삼성전자주식회사  
Applicant(s)



199 8 년 12 월 9 일

특 허 청  
COMMISSIONER



## 특허출원서

【출원번호】 98-039809

【출원일자】 1998/09/24

【발명의 국문명칭】 디지털 정보의 저작권 보호를 위한 프로토콜 포맷 및 프로토콜 포맷 처리 시스템

【발명의 영문명칭】 Protocol format for the authors' association protection and protocol format processing system

### 【출원인】

【국문명칭】 삼성전자 주식회사

【영문명칭】 Samsung Electronics Co., Ltd.

【대표자】 윤종용

【출원인코드】 14001979

【출원인구분】 국내상법상법인

【우편번호】 442-742

【주소】 경기도 수원시 팔달구 매탄3동 416번지

【국적】 KR

### 【대리인】

【성명】 윤의섭

【대리인코드】 H351

【전화번호】 02-564-7734

【우편번호】 135-080

【주소】 서울특별시 강남구 역삼동 823-24

### 【발명자】

【국문성명】 강은성

【영문성명】 KANG, Eun Seong

【주민등록번호】 641026-1067014

【우편번호】 137-069

【주소】 서울특별시 서초구 방배본동 삼호아파트 1-103

【국적】 KR

### 【발명자】

【국문성명】 변진영

【영문성명】 BYUN, Jin Young

【주민등록번호】 670423-2670417

【우편번호】 135-120

【주소】 서울특별시 강남구 신사동 599-4 압구정빌딩 소프트웨어센터

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다.

대리인

윤의섭 (인)

【심사청구】 특허법 제60조의 규정에 의하여 위와 같이 출원심사를 청구합니다.

대리인

윤의섭 (인)

【수신처】 특허청장 귀하

【수수료】

【기본출원료】 17 면 29,000 원

【가산출원료】 0 면 0 원

【우선권주장료】 0 건 0 원

【심사청구료】 5 항 269,000 원

【합계】 298,000 원

【첨부서류】 1. 요약서, 명세서(및 도면) 각 1통

2. 출원서 부분, 요약서, 명세서(및 도면)을 포함하는 FD부분 1통

3. 위임장(및 동 번역문)

## 【요약서】

### 【요약】

개시된 본 발명은 사용자의 고유문자열에 대응하여 생성된 암호화키에 따라 헤더, 암호화 규칙을 갖는 필드, 암호화된 디지털 정보 필드로 이루어진 전송포맷을 생성하고, 생성된 전송포맷을 사용자에게 전송하여 사용자로 하여금 전송된 포맷을 해독할 수 있도록 하는 디지털 정보의 저작권 보호를 위한 프로토콜 포맷 및 프로토콜 포맷 처리 시스템에 관한 것이다.

본 발명은 암호화 규칙 등의 암호화를 위한 정보가 들어 있는 헤더와 헤더의 정보에 따라 암호화된 디지털 정보로 이루어진 몸체로 구성된 디지털 정보 저작권 보호 프로토콜 포맷이 있으며, 디지털 정보를 상술한 디지털 정보 저작권 보호 프로토콜 포맷으로 변환하는 프로토콜 포맷 인코딩부와, 디지털 정보 저작권 보호 프로토콜 포맷 인코딩부에서 입력받은 프로토콜 포맷을 헤더의 정보에 따라 해독하는 디지털 정보 저작권 보호 프로토콜 포맷 디코딩부로 구성된다.

따라서, 본 발명은 네트워크를 통해 유료용 디지털 정보를 서비스 받고자 하는 사용자의 고유문자열에 대응하는 암호화키를 서버에서 생성하고, 생성된 암호화키에 의해서만 유료용 디지털 정보를 다운로드 하여 이용할 수 있도록 함으로써, 유료용 디지털 정보의 무분별한 복제를 미연에 방지할 수 있다는 효과를 제공하는 데 있다.

### 【대표도】

도 5

## 【명세서】

### 【발명의 명칭】

디지털 정보의 저작권 보호를 위한 프로토콜 포맷 및 프로토콜 포맷 처리 시스템

### 【도면의 간단한 설명】

도 1은 본 발명인 디지털 정보 전송시스템의 디지털 정보 복제 방지장치의 구성을 설명하기 위한 개략적인 블록도,

도 2는 본 발명인 디지털 정보 전송시스템의 디지털 정보 복제 방지장치의 다른 실시 예를 설명하기 위한 개략적인 블록도,

도 3은 도 1에 적용된 서비스 서버에서의 디지털 정보의 무단 복제를 방지하기 위한 방법을 설명하기 위한 동작 흐름도,

도 4는 도 2에 적용된 호스트 서버에서의 암호화키를 생성하고, 송신하는 방법을 설명하기 위한 동작 흐름도,

도 5는 본 발명인 프로토콜 포맷 처리 시스템의 구성을 설명하기 위한 도면,

도 6은 본 발명인 디지털 정보의 저작권 보호를 위한 프로토콜 포맷을 도시한 도면,

도 7은 도 6에 적용된 헤더부분을 도시한 도면,

도 8은 도 7에 적용된 암호화되지 않은 헤더부분을 도시한 도면이다.

\*도면의 주요부분에 대한 부호설명\*

10, 20 : 단말장치

11, 21 : 기록재생장치

12, 22 : 서비스 서버

23 : 호스트 서버

14, 24 : 서비스 결제대행 서버

50 : 프로토콜 포맷 인코딩부

51 : 프로토콜 포맷 디코딩부

#### 【발명의 상세한 설명】

#### 【발명의 목적】

#### 【발명이 속하는 기술분야 및 그 분야의 종래기술】

본 발명은 디지털 정보의 저작권 보호를 위한 프로토콜 포맷 및 프로토콜 포맷 처리 시스템에 관한 것이다.

보다 상세하게는 서버에서 사용자의 고유문자열에 대응하여 생성된 암호화키에 따라 헤더, 암호화 규칙을 갖는 필드, 암호화된 디지털 정보 필드로 이루어진 전송포맷을 생성하고, 생성된 전송포맷을 사용자에게 전송하여 사용자로 하여금 전송된 포맷을 해독할 수 있도록 하는 디지털 정보의 저작권 보호를 위한 프로토콜 포맷 및 프로토콜 포맷 처리 시스템에 관한 것이다.

최근 사람들은 방송, 출판 등과 같은 각종 미디어를 통해 공급되는 정보의 홍수 속에 살고 있다.

그러므로, 각종 미디어를 통해 공급되고 있는 정보를 통합하여 한꺼번에 공급하고자 하는 공급자가 생겨났으며, 공급자에 의해 공급되는 정보 중 원하는 정보만을 선택적으로 공급받고자 하는 사용자가 생기게 되었다.

이에 따라 각종 정보를 디지털 정보로 변환한 후 이 디지털 정보를 각각의

사용자에게 공급할 수 있도록 저장하는 공급자와, 네트워크(Network)를 통해 공급자로부터 정보를 공급받는 사용자로 이루어진 디지털 정보 전송시스템들이 출현하게 되었다.

이와 같은 디지털 정보 전송시스템은 사용자에게 디지털 정보를 손쉽게 다운로드 받을 수 있는 응용프로그램을 공급하게 되었고, 사용자는 네트워크에 의해 디지털 정보 전송시스템과 연결되어 있으므로 응용프로그램을 통해 사용자가 다운로드 받고자 하는 정보를 모두 얻을 수 있게 되었다.

상술한 디지털 정보 전송시스템에서 공급하고 있는 디지털 정보는 무료 또는 유료로 사용자에게 공급되는데, 유료로 공급되는 디지털 정보는 디지털 정보를 공급하는 디지털 정보 전송시스템을 갖는 서버가 각 디지털 정보에 대한 서비스 요금을 정하게 된다.

이렇게 서비스 요금이 정해진 디지털 정보를 사용자가 다운로드 받게 되면 서비스 서버는 사용자의 정보 이용량에 따라 서비스 요금을 누적시켜 사용자에게 부과하는 것이다.

그러나, 네트워크를 이용하여 상업적으로 디지털 정보를 제공하는 서버로 사용자가 접속해서 유료용 디지털 정보를 전송받는 경우 대부분의 사용자가 복제형식으로 다른 사람에게 무단으로 배포하거나 또는 복제된 디지털 정보를 얻어 사용하게 되는데, 이때 디지털 정보 전송시스템을 갖는 서버는 그 피해가 크나 이를 근본적으로 방지할 수 없다는 문제점이 있었다.

**【발명이 이루고자 하는 기술적 과제】**



따라서, 본 발명의 목적은 전술한 문제점을 해결할 수 있도록 서버에서 사용자의 고유문자열에 대응하여 생성된 암호화키에 따라 헤더, 암호화 규칙을 갖는 필드, 암호화된 디지털 정보 필드로 이루어진 전송포맷을 생성하고, 생성된 전송포맷을 사용자에게 전송하여 사용자로 하여금 전송된 포맷을 해독할 수 있도록 하는 디지털 정보의 저작권 보호를 위한 프로토콜 포맷 및 프로토콜 포맷 처리 시스템에 관한 것이다.

#### 【발명의 구성 및 작용】

이와 같은 목적을 달성하기 위한 본 발명은 암호화 규칙 등의 암호화를 위한 정보가 들어 있는 헤더와 헤더의 정보에 따라 암호화된 디지털 정보로 이루어진 몸체로 구성된 디지털 정보 저작권 보호 프로토콜 포맷이 있으며, 디지털 정보를 상술한 디지털 정보 저작권 보호 프로토콜 포맷으로 변환하는 프로토콜 포맷 인코딩부와, 디지털 정보 저작권 보호 프로토콜 포맷 인코딩부에서 입력받은 프로토콜 포맷을 헤더의 정보에 따라 해독하는 디지털 정보 저작권 보호 프로토콜 포맷 디코딩부로 구성됨을 특징으로 한다.

이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시 예를 상세히 기술하기로 한다.

도 1은 본 발명인 디지털 정보 전송시스템의 디지털 정보 복제 방지장치의 구성을 설명하기 위한 개략적인 블록도로서, 그 구성은 다음과 같다.

단말장치(10)는 사용자에게 회원 등록을 요청함과 동시에 사용자가 입력한 고유문자열을 서비스 서버(20)로 전송하고, 사용자에게 의해 요청되어 수신된 암호화

키를 저장하며, 서비스 서버(20)로부터 암호화된 디지털 정보를 다운로드 받아 암호화키에 의해 해독한다.

상술한 단말장치(10)에 저장된 암호화키는 회원 신규 가입시 사용자의 요청에 따라 사용자의 고유문자열에 대응하여 생성된 후 사용자에게 공급되는 것으로, 회원해지 신청을 하지 않는 이상 사용자가 다운로드 받고자 하는 디지털 정보는 상술한 암호화키를 이용하여 암호화된 후 네트워크를 통해 사용자의 단말장치(10)로 공급된다.

상술한 단말장치(10)는 도면에 도시된 바와 같이 일반 통신장치가 구비된 PC(11a)와 PC(11a)를 통해 암호화키를 전송받아 저장한 후 암호화된 디지털 정보를 전송받아 저장매체에 기록시키고, 저장된 암호화키를 이용하여 디지털 정보를 해독하여 재생하는 기록재생장치(11b)로 구성될 수 있다.

상술한 기록재생장치(11b)는 저장매체의 종류에 따라 휴대용 또는 거치형이 존재한다.

또한, 상술한 단말장치(10)는 통신이 가능한 장치이며, 무엇이든 무방한데 예를 들면 셀룰라폰, 디지털 TV 등과 같은 제품이다.

서비스 서버(12)는 단말장치(10)로부터 전송되는 고유문자열에 대응하는 암호화키를 생성하여 고유문자열과 함께 저장하고, 사용자가 암호화키를 요청하는 경우 이를 단말장치(10)로 송신하며, 디지털 정보 리스트를 가지 있어 사용자가 요청한 디지털 정보를 암호화키와 암호화 알고리즘에 따라 암호화한 후 단말장치(10)로 다운로드 되도록 한다.

서비스 결제대행 서버(13)는 상술한 서비스 서버(12)로부터 사용자의 요구에 따라 디지털 정보를 다운로드 시킨 후 발생하는 비용에 대한 신호를 수신받아 등록된 사용자의 ID에 디지털 정보 서비스 요금을 누적시켜 사용자에게 청구하게 된다.

이때, 상술한 고유문자열은 사용자가 서비스 서버에 등록할 경우 입력하는 사용자의 주민등록번호가 대부분이나, 운전면허번호와 같이 사용자를 유일하게 구별할 수 있는 문자열이면 어느 것이든지 사용 가능하다.

도 2는 본 발명인 디지털 정보 전송시스템의 디지털 정보 복제 방지장치의 다른 실시 예를 설명하기 위한 개략적인 블록도로서, 본 발명의 일 실시예인 도 1에서 설명한 것과 동일한 부분인 단말장치(20), 기록재생장치(21), 서비스 결제 서버(24)에 대해서는 그 설명을 생략하기로 한다.

서비스 서버(22)는 상술한 단말장치(20)로부터 전송되는 고유문자열에 대응하는 암호화키를 요청받기 위한 신호를 후술할 호스트 서버(23)로 송신하고, 이에 따라 호스트 서버(23)로부터 암호화키를 전송받아 단말장치(20)로 송신하게 된다. 또한, 서비스 서버(22)는 디지털 정보 리스트를 가지 있어 사용자가 요청한 디지털 정보를 암호화키를 이용하여 암호화시킨 후 단말장치(20)로 다운로드되도록 한다.

호스트 서버(23)는 상술한 서비스 서버(22)로부터 송신되는 고유문자열에 대응하는 암호화키를 생성하여 고유문자열과 함께 저장한 후 서비스 서버(22)의 요청 신호에 따라 암호화키를 서비스 서버(22)로 전송한다.

이와 같이 구성된 본 발명에 따른 디지털 정보 전송시스템의 디지털 정보 복제 방지장치의 동작을 첨부한 도면을 참조하여 좀 더 구체적으로 설명한다.

도 3은 도 2에 적용된 서비스 서버에서의 디지털 정보의 무단 복제를 방지하기 위한 방법을 설명하기 위한 동작 흐름도이다.

도시된 바와 같이, 서비스 서버(22)는 단말장치(20)를 이용해 사용자가 회원등록을 신청하기 위한 신호를 입력하였는지를 판단(S101)하고, 판단 결과 회원등록을 신청하기 위한 신호가 입력된 경우, 사용자가 단말장치(20)를 이용하여 입력한 고유문자열이 수신되는지를 판단(S102)한다.

상술한 단계(S102)의 판단 결과, 단말장치(20)로부터 고유문자열이 수신되는 경우 수신된 고유문자열에 의해 회원인지 신규가입자인지를 판단(S103)하고, 판단 결과 신입가입자인 경우 서비스 서버(22)는 사용자에게 회원정보를 입력할 수 있는 메시지를 출력하고, 그에 따라 입력된 회원등록정보를 수신받아 저장(S104)한다.

한편, 상술한 단계(S101)의 판단 결과, 사용자로부터 회원등록을 신청하기 위한 신호가 입력되지 않은 경우 또는 단계(S102)의 판단 결과 사용자로부터 고유문자열이 입력되지 않는 경우 사용자가 선택한 다른 메뉴에 따라 디지털 정보 전송 시스템의 진행모드가 변경(S140)된다.

상술한 단계(S104)에서 서비스 서버(22)가 회원등록정보를 저장한 후에는 단말장치(20)로부터 암호화키를 송신받고자 하는 요청신호가 수신되는지를 판단(S105)하고, 단계(S105)의 판단 결과 암호화키를 송신받고자 하는 요청신호가 수신되는 경우 서비스 서버(22)는 사용자의 고유문자열에 해당되는 암호화키를 생성한 후 사용자에게 송신(S106)함으로써, 서비스 서버(22)에서 공급하는 유료용 디지털 정보를 다운로드 받기 위한 모든 단계(S100)의 동작이 완료되는 것이다. 상술한 단

계(S100)의 동작수행은 사용자가 회원가입을 해지하지 않는 경우에는 사용자의 고유문자열에 따라 암호화키가 생성, 유지된다.

또한, 상술한 단계(S103)에서 사용자가 입력한 고유문자열이 등록된 고유문자열인 경우 이미 암호화키를 가지고 있는 사용자로 판단하여 후술할 디지털 정보에 대한 사용자로부터 다운로드 요청신호가 수신되는지를 판단하는 단계(S110)부터 수행하게 되며, 전술한 단계(S104)에서 단계(S106)까지 수행되는 과정은 신입가입자에 대해서만 이루어진다.

상술한 단계(S106) 수행 후 단말장치(20)로부터 디지털 정보에 대한 다운로드 요청신호가 수신되는지를 판단(S110)하고, 판단 결과 다운로드 요청신호가 수신되는 경우 서비스 서버(22)가 생성한 암호화키 또는 호스트 서버(23)에 의해 생성된 암호화키를 수신받아 사용자가 다운로드 받고자 하는 디지털 정보를 암호화한 후 사용자에게 송신(S120)한다.

또한, 서비스 서버(22)는 사용자에게 암호화된 디지털 정보를 전송(S120)후 발생하는 서비스 요금을 서비스 결제대행 서버(24)로 전송(S130)하여 저장된 요금에 누적되도록 한다. 그러면 서비스요금 결제대행 서버(24)는 사용자가 디지털 정보를 이용하는데 대한 서비스요금을 누적한 후 청구서를 사용자에게 발송하게 되는 것이다.

도 4는 도 2에 적용된 호스트 서버에서의 암호화키를 생성하고, 송신하는 방법을 설명하기 위한 동작 흐름도이다.

도시된 바와 같이, 호스트 서버(23)는 서비스 서버(22)로부터 고유문자열이

수신되는지를 판단(S400)하고, 판단 결과 수신된 고유문자열과 저장된 고유문자열을 비교하여 동일한 고유문자열이 있는지를 판단(S410)한다.

상기 단계(S410)의 판단결과, 동일한 고유문자열이 있는 경우 고유문자열과 함께 저장된 암호화키를 서비스 서버(22)로 전송(S420)하고, 동일한 고유문자열이 없는 경우 암호화키를 생성(S430)한 후 생성된 암호화키와 함께 사용자 ID 및 고유문자열을 저장(S440)한다.

이때, 상술한 서비스 서버(22)에서 수행되는 단계(S106) 및 호스트 서버(23)에서 수행되는 단계(S400~S440)는 도 2에 도시된 바와 같이 서비스 서버(22)와 호스트 서버(23)가 따로 구비된 경우에 수행되는 과정이나, 도 1에 도시된 바와 같이 서비스 서버(11)만이 구비된 경우에는 서비스 서버(11)에서 상술한 단계가 통합적으로 수행되어 사용자의 고유문자열에 대응하여 암호화키를 생성하고, 생성된 암호화키를 사용자에게 전송하게 되며, 이에 대한 동작 흐름도를 도시하지 않았으나 도 3 및 도 4에 미루어 그 동작을 이해할 수 있으므로 그 설명은 생략하기로 한다.

도 5는 본 발명인 프로토콜 포맷 처리 시스템의 구성을 설명하기 위한 도면으로서, 도시된 바와 같이 디지털 정보의 저작권 보호를 위한 프로토콜을 생성하는 프로토콜 포맷 인코딩부(50)와, 상기 저작권 보호 프로토콜 포맷 인코딩부(50)로부터 입력받은 프로토콜 포맷을 헤더의 정보에 따라 디지털 정보를 재생하는 저작권 보호 프로토콜 포맷 디코딩부(51)로 구성된다.

도 6은 본 발명인 디지털 정보의 저작권 보호를 위한 프로토콜 포맷을 도시한 도면으로서, 도시된 바와 같이 상술한 디지털 정보의 저작권 보호를 위한 프로

토콜 포맷은 헤더와 암호화된 디지털 정보로 이루어진 몸체로 이루어진다.

도 7은 도 6에 적용된 헤더부분을 도시한 도면으로서, 도시된 바와 같이 상술한 디지털 정보의 저작권 보호를 위한 프로토콜 포맷에서 헤더는 몸체가 저작권을 지원하는 정보로 이루어진지를 설명하기 위한 필드, 암호화되지 않은 헤더의 크기를 설명하기 위한 필드, 암호화되지 않는 헤더, 암호화된 헤더의 크기를 설명하기 위한 필드, 암호화된 헤더로 이루어진다.

도 8은 도 7에 적용된 암호화되지 않은 헤더부분을 도시한 도면으로서, 도시된 바와 같이 상술한 암호화되지 않은 헤더는 저작권 보호 프로토콜의 버전에 대한 필드, 디지털 정보의 포맷에 대한 필드, 디지털 정보 제공자의 코드에 대한 필드, 사용자의 고유문자열을 암호화하는데 사용하는 알고리즘의 코드에 대한 정보 필드, 단말장치에서 공유하는 사용자의 수 및 각 사용자의 고유문자열에 대한 필드, 기록 재생수단에서 공유하는 사용자의 수 및 각 사용자의 고유문자열에 대한 필드로 이루어진다.

#### 【발명의 효과】

따라서, 상술한 바와 같이 본 발명은 네트워크를 통해 유료용 디지털 정보를 서비스 받고자 하는 사용자의 고유문자열에 대응하는 암호화키를 서버에서 생성하고, 생성된 암호화키에 의해서만 유료용 디지털 정보를 다운로드하여 이용할 수 있도록 함으로써, 유료용 디지털 정보의 무분별한 복제를 미연에 방지할 수 있다는 효과를 제공하는데 있다.

**【특허청구범위】**

**【청구항 1】**

디지털 정보의 저작권 보호를 위한 프로토콜을 생성하는 프로토콜 포맷 인코딩 수단; 및

상기 저작권 보호 프로토콜 포맷 인코딩수단으로부터 입력받은 프로토콜 포맷을 헤더의 정보에 따라 디지털 정보를 재생하는 저작권 보호 프로토콜 포맷 디코딩수단으로 구성된 것을 특징으로 하는 프로토콜 포맷 처리 시스템

**【청구항 2】**

헤더와 암호화된 디지털 정보로 이루어진 몸체로 구성된 것을 특징으로 하는 디지털 정보의 저작권 보호를 위한 프로토콜 포맷.

**【청구항 3】**

제 2 항에 있어서, 상기 저작권 보호 프로토콜 포맷은 부가정보필드를 더 포함하여 이루어지는 것을 특징으로 하는 디지털 정보의 저작권 보호를 위한 프로토콜 포맷.

**【청구항 4】**

제 2 항에 있어서, 상술한 디지털 정보의 저작권 보호를 위한 프로토콜 포맷에서 헤더는;

몸체가 저작권을 지원하는 정보로 이루어진지를 설명하기 위한 필드, 암호화되지 않은 헤더의 크기를 설명하기 위한 필드, 암호화되지 않는 헤더, 암호화된 헤더의 크기를 설명하기 위한 필드, 암호화된 헤더로 구성됨을 특징으로 하는 디지털



정보의 저작권 보호를 위한 프로토콜 포맷.

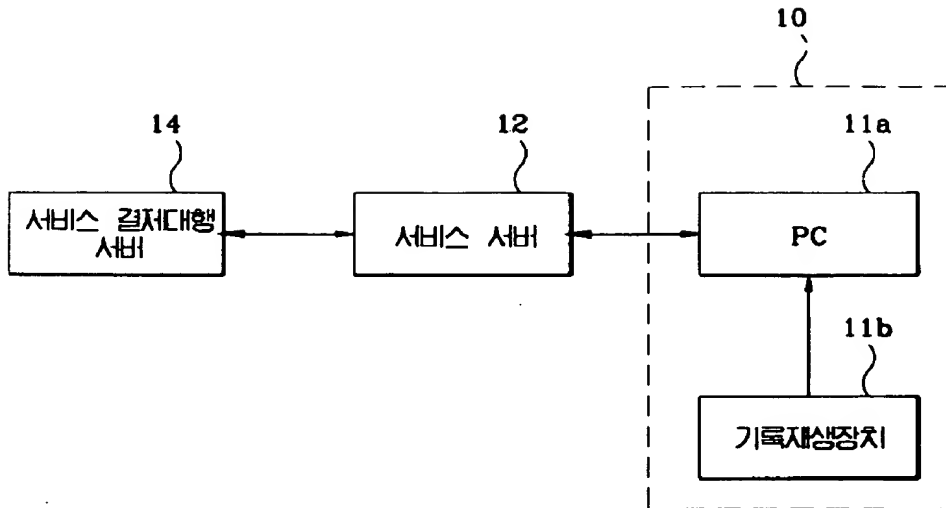
【청구항 5】

제 4 항에 있어서, 상기 암호화되지 않은 헤더는;

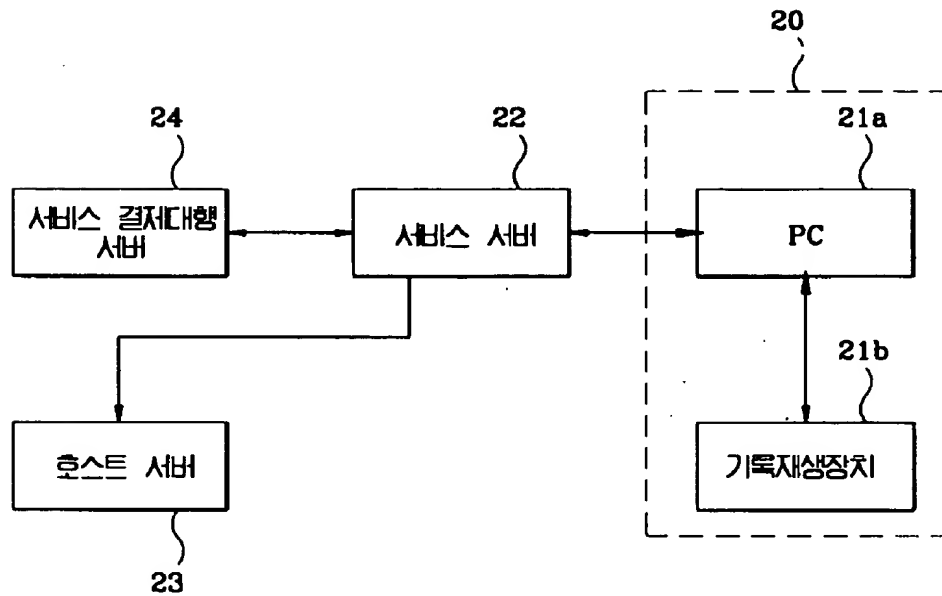
저작권 보호 프로토콜의 버전에 대한 필드, 디지털 정보의 포맷에 대한 필드, 디지털 정보 제공자의 코드에 대한 필드, 사용자의 고유문자열을 암호화하는데 사용하는 알고리즘의 코드에 대한 정보 필드, 단말장치에서 공유하는 사용자의 수 및 각 사용자의 고유문자열에 대한 필드, 기록재생수단에서 공유하는 사용자의 수 및 각 사용자의 고유문자열에 대한 필드로 이루어짐을 됨을 특징으로 하는 디지털 정보의 저작권 보호를 위한 프로토콜 포맷.

【도면】

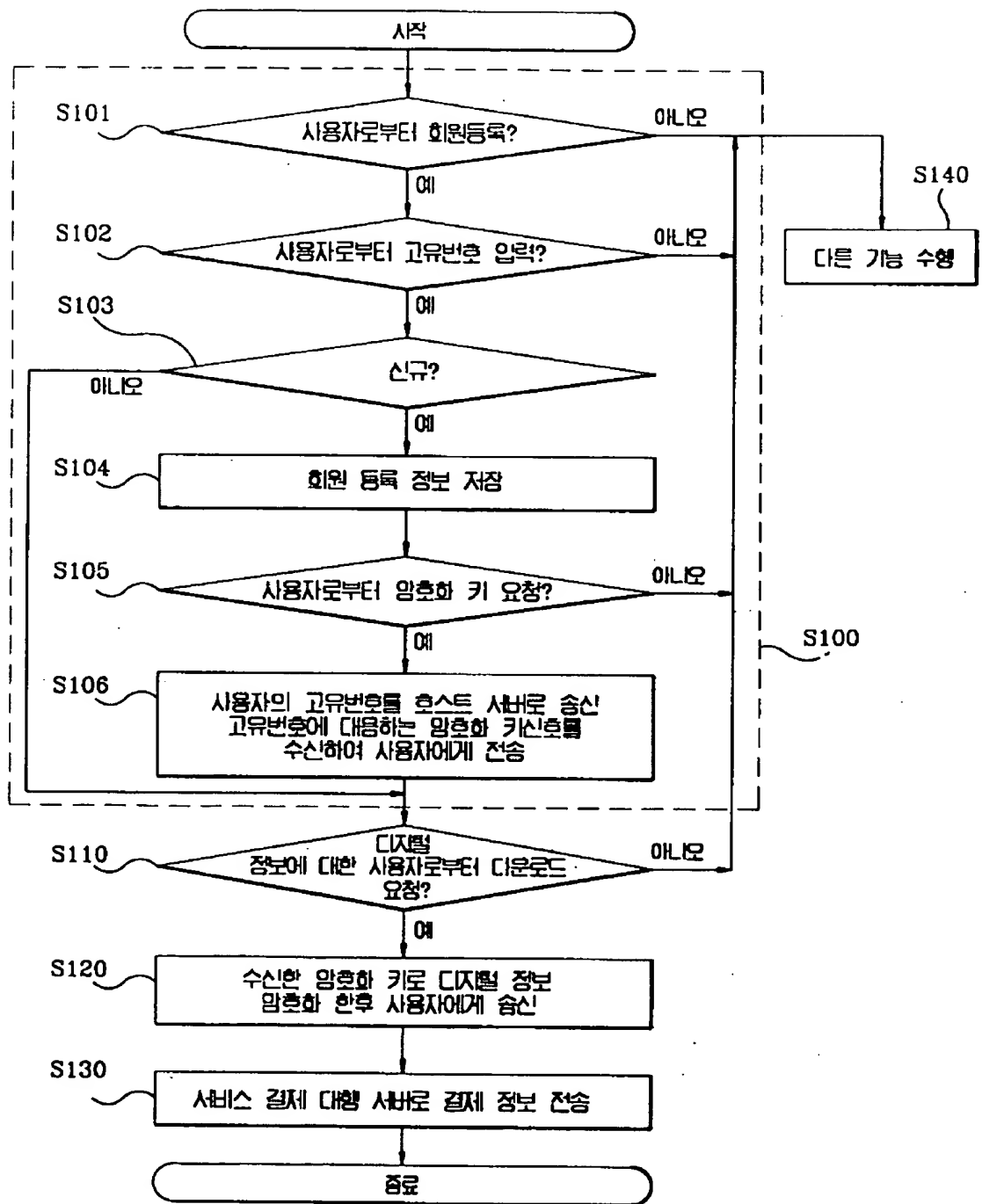
【도 1】



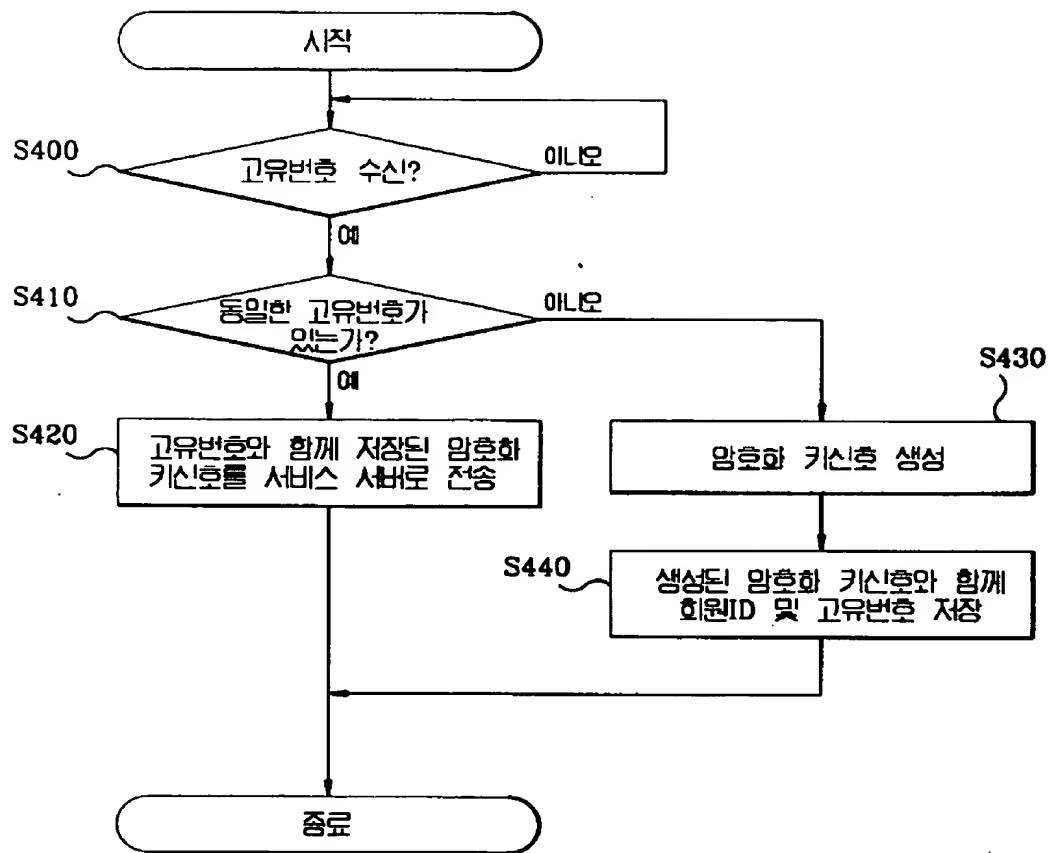
【도 2】



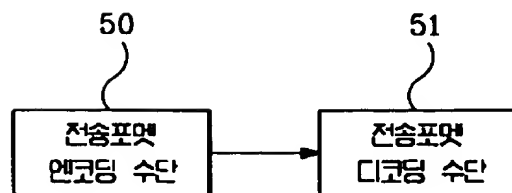
【도 3】



【도 4】



【도 5】



【도 6】

헤더	암호화된 디지털 정보 의 크기	암호화된 디지털 정보	부가정보
----	---------------------	-------------	------

【도 7】

저작권 지원정보	암호화 되지 않은 헤더의 크기	암호화 되지 않은 헤더	암호화된 헤더의 크기	암호화된 헤더
----------	---------------------	-----------------	----------------	------------

【도 8】

저작권 라이브러리 버전	디지털 변환 포맷	디지털 정보 제공자의 코드	고유번호를 암호화하는 알고리즘 코드	PC공유 사용자수 및 고유번호	가독제생장장치에서 공유 사용자수 및 고유번호
-----------------	--------------	-------------------	------------------------	---------------------	-----------------------------